REMARKS

CLAIM REJECTIONS – 35 USC § 102 & § 103

Claims 1, 6, 7, 12, and 18 are rejected under 35 U.S.C. 102(b) as being taught by Huuhtanen et al. (European Patent Publication EP 0 674 441 A1; hereinafter "Huuhtanen"). Claims 2-5, 8-11, 13-16, and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Huuhtanen in view of Pasqualino (US Publication No. 2002/0163598 A1; hereinafter "Pasqualino").

Accordingly, independent claims 1, 6, and 12 have been amended to further clarify the distinction between the present application and the cited references. It is respectfully submitted that the cited references, either individual or in combination, do not disclose every limitation recited in amended independent claims 1, 6, and 12. More specifically, with respect to claim 1, it is respectfully submitted that the cited references do no disclose using *multiple and different* encryption/decryption keys to encrypt/decrypt different groups of *related* data packets that are transmitted *during a single transmission*, and that *all* the data packets are encrypted before transmission. (See claim 1, "forming a first group of encrypted data packets…; forming a second group of encrypted data packets…; transmitting the encrypted data packets…; decrypting the first group of encrypted data packets…; decrypting the second group of encrypted data packets.") In other words, data packets encrypted using *different* encryption keys *are transmitted together*.

First, with Huuhtanen, *not all* data packets to be transmitted are scrambled before transmission. In fact, Huuhtanen specifically states that, "it is essential that some of the data packets related to a particular program are scrambled and some are transmitted without scrambling." (See Huuhtanen, Abstract.) In the various embodiments different methods of selecting some data packets to be scrambled and some data packets not to be scrambled are described. For example, in the first embodiment, packets to be scrambled are selected in a predetermined manner (see Huuhtanen, col. 5, lines 40-46). In the second embodiment, packets to be scrambled are selected at random intervals (see Huuhtanen, col. 6, lines 42-45). In the third embodiment, packets to be scrambled are selected based on time (see Huuhtanen, col. 7, lines

25-29). And so on. In each and every embodiment, *some data packets are selected to be scrambled, while the unselected data packets are left unscrambled.*

In contrast, with the present application, *all data packets* are encrypted before transmission. Independent claims 1, 6, and 12 have been amended to specifically recite that *each and every one of the data packets formed at the source device is encrypted.*

Next, the outstanding office action, on page 2, indicates that because Huuhtanen teaches multiple description keys, it implies that there are multiple encryption keys. Huuhtanen, at col. 6, lines 24-35 & 49-55 and col. 7, lines 33-37, discloses having decryption keys. In addition, Fig. 10 shows a key set 22 and Fig. 11 shows a key set 32, both including encryption keys. (See also, Huuhtanen, col. 9, lines 15-17 & 40-47.)

However, although Huuhtanen discloses multiple encryption/decryption keys, Huuhtanen does not specifically disclose using multiple encryption/decryption keys to encrypt/decrypt different groups of *related* data packets *that are transmitted together during a single transmission*.

Often, an encryption/decryption system has multiple encryption/decryption keys to achieve better security protection. The keys used vary among *different transmissions*. For example, during one transmission, the system may select one pair of encryption/decryption key to encrypt/decrypt all the data packets sent during that specific transmission. Then, during another transmission at a different time, the system may select another pair of encryption/decryption key to encrypt/decrypt all the data packets sent during that second specific transmission. Thus, even when a system has multiple encryption/decryption keys, *it does not necessarily imply that multiple encryption/decryption keys are used during the same single transmission*.

With Huuhtanen, although data packets from one program may be scrambled with one encryption key while data packets from another program may be scrambled with a different encryption key, *data packets belonging to the same program are scrambled with the same encryption key*.

In contrast, with the present application, two or more pairs of encryption/decryption keys, i.e., encryption/decryption values, are used to encrypt/decrypt *related* data packets during the

same transmission. The data packets are related in the sense that they belong to the same program. More specifically, one encryption key is used to encrypt one group of data packets, and at least another, different encryption key is used to encrypt at least another, different group of data packets. The two or more groups of data packets, encrypted using different encryption keys, i.e., the encryption values, are transmitted together. Subsequently, at their destination, the two or more groups of data packets are decrypted using multiple, different decryption keys, each corresponding to their respective encryption key. Independent claims 1, 6, and 12 have been amended to further clarity that the number of data packets formed at the source device are related.

It would not have been obvious to determine using multiple encryption/decryption keys during a single transmission from the cited references, because nothing in the cited references teaches or suggests how to select an appropriate decryption key to decrypt a particular data packet at the destination, when the data packet may have been encrypted with one of several encryption keys. In other words, the cited references do not teach or suggest how to match and select a decryption key with the corresponding encryption key used with respect to a particular data packet when there are multiple possibilities. In contrast, as recited in amended independent claim 1, the first set of decryption values used to decrypt the first group of encrypted data packets corresponds to the first set of encryption values, and the second set of decryption values used to decrypt the second group of encrypted data packets corresponds to the second set of encryption values.

For above reasons, amended independent claim 1 is patentably distinct from the cited references. Independent claims 6 and 12 recite similar limitations and are therefore patentably distinct from the cited references for the same reasons as applied to claim 1.

Dependent claim 19 has been cancelled.

Dependent claims 2-5, 7-11, 13-16, 18, and 20 directly or indirectly depend from claims 1, 6, and 12, and are therefore respectfully submitted to be patentable over the art of record for at least the reasons set forth above with respect to the independent claims. Further, these dependent claims recite additional limitations that when considered in the context of the claimed invention further patentably distinguish the art of record.

CONCLUSION

In view of the foregoing amendments and remarks, it is respectfully submitted that the claimed invention as presently presented is patentable over the art of record and that this case is now in condition for allowance. Accordingly, the Applicants request withdrawal of all pending rejections and request reconsideration of the pending application and prompt passage to issuance. As an aside, the Applicants clarify that any lack of response to any of the issues raised by the Examiner is not an admission by the Applicants as to the accuracy of the Examiner's assertions with respect to such issues. Accordingly, Applicants specifically reserve the right to respond to such issues at a later time during the prosecution of the present application, should such a need arise.

As always, the Examiner is cordially invited to telephone the Applicants' representative to discuss any matters pertaining to this case. Should the Examiner wish to contact the undersigned for any reason, the telephone number set out below can be used.

If any fees are due in connection with the filing of this Amendment, the Commissioner is authorized to deduct such fees from the undersigned's Deposit Account No. 50-4481 (Order No. GENSP047).

Respectfully submitted,
BEYER LAW GROUP LLP

/Bernadette Lee/
Bernadette Lee
Registration No. 60,298

P.O. Box 1687
Cupertino, CA 95015-1687
(408) 255-8001